REMARKS

This Amendment is in response to the Office Action dated December 4, 2006. In the Office Action, claims 2, 5, 11-19 and 22-25 were rejected under 35 USC §112 and claims 1-25 were rejected under 35 USC §102. By this Amendment, claims 1, 2, 4-6, 9, 10 and 19-21 are amended, and claims 11-18 and 22-25 are cancelled.

CLAIM OBJECTIONS:

Claim 10 was objected because of a typographical error in the claim. By this amendment, the word "secrete" is replaced with "secret". The Applicants thank the Examiner for finding this error.

CLAIM REJECTIONS UNDER 35 USC §112:

Claim 2

Claim 2 was rejected under 35 USC §112, second paragraph, as allegedly being indefinite for failing to particularly out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner states, "It is indefinite as to how the sent information will get to a receiver if a target isn't specified." OA, pg. 2-3.

35 USC §112, second paragraph, requires, "The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." A rejection based on the failure to satisfy this requirement is appropriate only where applicant has stated, somewhere other than in the application as filed, that the invention is something different from what is defined by the claims. MPEP 2172.

As discussed in the detailed description of the invention, information from the provider terminal can be distributed to user terminals in a number of ways without knowing the specific user terminals that is to receive the information. For example, the provider terminal can use an electronic mail distribution service by specifying attributes of recipients of the mail without knowing who has the specified attributes. App., par. [0107]-[0108]. In another embodiment, a distributed matching service is utilized to exchange information without revealing user terminal identities. App., par. [0110]. Yet anther embodiment of the present invention employs a community key generation method which, instead of directly specifying the addresses of user terminals, a combination of attributes is specified as criteria to allow only those who meet the criteria to receive the content while preventing leakage of personal attribute information to third parties, including the provider terminal. App, par. [0115].

Thus, it is respectfully submitted that claims 2, 5, and 19 do particularly pointing out and distinctly claiming the subject matter of the Applicants' invention.

Claims 11-18 and 22-25

Claims 11-18 and 22-25 were rejected as dependent on a different type of invention. By this amendment, claims 11-18 and 22-25 are cancelled and their rejections are therefore moot.

Claim 19

Claim 19 was rejected because the Examiner alleged that it is indefinite how variables k and n relate to the keys. OA, pg. 3. By this amendment, claim 19 expressly recites, "n is the number of secret keys and public keys, and k is the number of the secret keys selected at random by the given client." This amendment is believed to overcome the rejection.

Claims 5 and 19

Claims 5 and 19 were rejected as dependent on a different type of invention. OA, pg. 3. Specifically, the Examiner alleges the term "oblivious transfer to generate" is unclear. Id.

By this amendment, claims 5 and 9 are amended to clarify that oblivious transfer ("OT") is a type of protocol. OT is a protocol by which a sender sends some information to the receiver, but remains oblivious as to what is sent. More information about this protocol is found in the present application at paragraphs [0062] to [0066].

Amended claims 5 and 19 make clear that oblivious transfer is a type of transfer protocol and therefore overcome the §112 rejections.

CLAIM REJECTIONS UNDER 35 USC §102:

Claims 1-25 were rejected as anticipated under 35 USC §102 by U.S. Patent No. 6,215,877 issued to Matsumoto ("Matsumoto"). OA, pg. 3. To anticipate a claim under 35 USC §102, a reference must teach every element of the claim. MPEP 2131.

Claim 1

Matsumoto relates to a chat system for performing real time communication. Matsumoto, col. 1, ln. 1-10. The system includes a key management server for generating a channel secret key unique to each communication channel for encrypting and decrypting the communication data exchanged through a plurality of channels managed by one or more chat servers. Matsumoto, col. 6, ln. 42-51. According to Matsumoto, by assigning a public key unique to the user from an external unit, communication can be kept secret even in the case where the reliability of the chat server is low. Matsumoto, col. 15, ln. 64-67.

Claim 1 is amended to recite, in part, "a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal." Support for this amendment can be found at least at paragraph [0045] of the pending application. It is respectfully submitted that Matsumoto does not teach or suggest attribute secret keys corresponding to attributes identifying a user terminal.

For at least this reason, claim 1 is believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claim 1.

Claim 2

Claim 2 recites, "The information distribution system according to claim 1, wherein said provider terminal distributes said encrypted content without specifying an address of said user terminal that is to receive said encrypted content." The applicants respectfully submit that Matsumoto is not concerned with keeping the addresses of recipients secret from provider terminals. Thus, claim 2 is not anticipated by Matsumoto.

Claim 3

Claim 3 is dependent on and further limits claim 1. Since claim 1 is believed allowable, claim 3 is also believed allowable for at least the same reasons as claim 1.

Claim 4

Claim 4 is amended to recite, in part, "wherein said attribute values identifying said user terminal." Support for this amendment can be found at least at paragraph [0045] of the pending application. It is respectfully submitted that Matsumoto does not teach or suggest attribute values identifying a user terminal.

For at least this reason, claim 4 is believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claim 4.

Claim 5

Claim 5 recites, "The server according to claim 4, wherein said attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer protocol." It is respectfully submitted that Matsumoto does not teach or suggest utilizing an oblivious transfer protocol.

For at least this reason, claim 5 is believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claim 5.

Claim 6

Claim 1 is amended to recite, in part, "a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes identifying a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys." Support for this amendment can be found at least at paragraph [0045] of the pending application. It is respectfully submitted that Matsumoto does not teach or suggest attribute values indicating attributes identifying a recipient to which a content is to be sent and using public keys to generate criteria keys that can be decrypted by secret keys corresponding to the public keys.

For at least this reason, claim 6 is believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claim 6.

Claims 7 and 8

Claims 7 and8 are dependent on and further limits claim 6. Since claim 6 is believed allowable, claims 7 and 8 are also believed allowable for at least the same reasons as claim 6.

Claim 9

Claim 9 is amended to recite, in part, "a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys." Support for this amendment can be found at least at paragraph [0045] of the pending application. It is respectfully submitted that Matsumoto does not teach or suggest receiving attribute secret keys corresponding to attributes established for identifying an information processing apparatus.

For at least this reason, claim 9 is believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claim 9.

Claim 10

Claim 10 is dependent on and further limits claim 9. Since claim 9 is believed allowable, claim 10 is also believed allowable for at least the same reasons as claim 9.

Claim 19

Claim 5 recites, in part, "reading said k secret keys corresponding to information about the obtained secret keys from said storage and using a protocol for implementing oblivious transfer protocol to generate decryption keys for decrypting information encrypted with said k public keys corresponding to the k secret keys." It is respectfully submitted that Matsumoto does not teach or suggest utilizing an oblivious transfer protocol.

For at least this reason, claim 19 is believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claim 19.

Claims 20 and 21

Claims 20 and 21 are amended to recite, in part, "attribute secret keys corresponding to attributes identifying the user terminals." As noted above, Matsumoto does not teach or suggest attribute secret keys corresponding to attributes identifying user terminals.

For at least this reason, claims 20 and 21 are believed allowable over the cited art. The Applicants respectfully request reconsideration and allowance of claims 20 and 21.

CONCLUSION

In view of the forgoing remarks, it is respectfully submitted that this case is now in condition for allowance and such action is respectfully requested. If any points remain at issue that the Examiner feels could best be resolved by a telephone interview, the Examiner is urged to contact the attorney below.

Applicants have amended claims 1, 2, 4-6, 9, 10 and 19-21 and cancelled claims 11-18 and 22-25 from further consideration in this application. Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the present claim amendments and cancellations are only for facilitating expeditious prosecution of the allowable subject matter noted by the examiner. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

No fee is believed due with this Amendment, however, should a fee be required please charge Deposit Account 50-0510. Should any additional extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: May 4, 2007

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (866) 607-8538